Verband der TÜV e.V.

TÜV®

Date
18 January 2017

Requirements for the telematics interface in vehicles

Trustworthy access to vehicle data and to data generated by vehicles

Executive Summary

The automatization and the interconnection of cars will increase in the future. It is crucial to provide a protection of the data of the consumers as well as a protection against cyberattacks and to establish equal conditions for all competitors with data-based business models.

In this respect the Association of Technical Inspection Agencies (VdTÜV e.V.) proposes a **security architecture (*automotive platform*)** in connected vehicles that comply with all these requirements.

This communication platform creates a uniform and interoperable standard for security and functional safety in the vehicle and protects it against unauthorized external access. Any information leaving the vehicle shall be processed in advance by the implemented platform in accordance with specific user profiles. The vehicle profiles can be modified by a neutral service provider (administrator). Due to data protection requirements this administrator has no direct read access to the data.

The *automotive platform* creates for all parties:

- **security by design**: the vehicle protects itself against external cyberattacks.
- **privacy by design**: data protection of the passengers is granted automatically by the implemented technology. The necessary data and application scenarios can be designed and modified in a flexible manner.
- **a tamper-proof technology**: Due to an embedded, highly *secure element* in the platform this technological approach is tamper-proof.

The automotive platform stands for:

- an improvement of **road safety** by using possibilities of the monitoring of safety- and emission related systems of the vehicle.
- **trustworthy administration of data** by an independent, neutral service provider that promotes free competition in the mobility sector.
- **a future proof solution** by highly secure and flexible update options and application scenarios like car-to-x communication.

The automotive platform approach of VdTÜV provides a trustworthy extended vehicle concept for all market players and consumers who appreciate data protection as well as *safety&security* as an added value for future connected vehicles.

1. Introduction

For more than 100 years, road safety and, for more than two decades, environmental protection have been drivers of more innovation, investment, growth and jobs in car manufacturing. Today, information technology is the key innovation driver of connected vehicles. The IT-induced change entails new challenges for the IT security against hacker attacks or viruses as well as for data protection based on the fact that all data generated by vehicles are personal data once being connected to the vehicle identification number or the license plate.

Digital platforms play the central role in the development of new business areas and employment opportunities. They collect data about vehicles and their users and process them in order to provide information and data-based services inside the vehicle. New digital platforms are increasingly calling into question existing value chains and legal relationships between the manufacturer, dealer, platform operator and third-party provider, on the one side, and the vehicle owner and vehicle user, on the other.

In collecting and processing data of machines, sensors and processes, the vehicle manufacturers take on a special position due to the fact that they develop the corresponding software and install it in the vehicle. Consequently, manufacturers have additional information and the technical knowledge to establish a direct connection to the vehicle user. With new services, such as the introduction of the automated emergency call system eCall which is mandatory from 2018, they can also offer a telematics and data service that brings measurable added value for customers (BMW – concierge service, GM/Opel – OnStar module, etc.). This added value includes assisting in the planning of journeys and in organising vehicle maintenance, keeping the software updated and creating new infotainment options.

Currently third-party providers do not have – or only with great difficulty – access to the data generated by connected vehicles. However, as the interconnection of cars will increase in the future, the data of the consumer must be protected. Furthermore, equal conditions have to be established for all competitors with data-based business models.

By establishing uniform and binding specifications and by implementing a uniform IT security standard for the future mode of data exchange via the vehicle's telematics interfaces, both goals can be achieved. In this respect the Association of Technical Inspection Agencies (VdTÜV) proposes a security architecture in connected vehicles which increases the protection from cyberattacks and improves data protection as well as creating a level playing field for all market players.

2. Fundamental data protection principles in connected cars

The top priority of a modern data policy must remain the protection of the right to privacy, of the fundamental right to the consumer empowerment and his freedom of choice. The appropriate information on the choices and their features are paramount to the vehicle owner/user.

In accordance with the recommendations of the 52nd German Conference on Road Traffic Law (*Deutscher Verkehrsgerichtstag*), the "exchange of data and information from the vehicle [should be subject to] rules [...] which ensure the right to informational self-determination through transparency and the freedom of choice of the person concerned (e.g. vehicle owners and drivers)". All automotive data is legally relevant. Under section 3 paragraph 1 of the German Data Protection Act *(Bundesdatenschutzgesetz)*, personal data means any information concerning the personal or material circumstances of an identified or identifiable individual. The data relating to the vehicle system, the operation and location as well as communication always contain information which can be matched to the owner at least, as this information relates to his or her vehicle. The challenge therefore is in providing consumers with comprehensive and full information. They need to relate to the data flow. On this basis only, the consumers are able to take a conscious decision upon the data that they wish to make accessible to be used and processed – and at what time, for what purpose, under which conditions and for which company.

To this end, it must be a political priority to making publically available the social and economic potential of data. Due to a combination of barriers to the free movement of data and many legal uncertainties regarding data, there is however no internal market for data. As a result, economic, social and business opportunities can't be pursued. Policy makers need to make sure that data migration doesn't stop at borders or industries, and that data can be accessed and re-used in the best possible way.

New vehicles are equipped with numerous sensors that analyze technical parameters and environmental conditions. They record a mixture of personal data, for example the positioning of the pedals or the steering angle and non-personal "raw" data for example rotational speeds of the wheels, engine performance and brake pressure that can be read via the OBD (on-board diagnosis) connector. Where automated data allows the identification of a natural person, it qualifies as personal data with the consequence that all rules on personal data codified in the General Data Protection Regulation apply until such data has been fully anonymized.

Accordingly, article 6 paragraph 9 lit. (i) of the eCall Directive sets out that the vehicle owners' personal data may only be processed with their "explicit consent". The directive also sets standards regarding the informing of the vehicle owners and/or users: In article 6 paragraph 9, it is stated that "manufacturers shall provide clear and comprehensive information in the owner's manual about the processing of data".

The property right to and the transmission of non-personal data is currently largely unregulated. For scientific purposes and the development of new digital business models, third parties shall have an open and secure access to this type of data at their own discretion. On one condition: They must have no way of connecting the data to a natural person.[1]

3. Requirements for security and safety in the vehicle

Modern automotive technology meets the highest demands in terms of functional vehicle safety (ABS, ESP, ACSF, etc.). By contrast, the protection of the vehicle's IT security is rather weak. Car manufacturers usually develop their own IT security systems which are not necessarily interoperable and so fail to adequately protect against malpractice and manipulation. In view of the above, VdTÜV calls for an appropriate specification of a uniform standardised solution. This would allow for manipulation and for remote attacks on the vehicle – particularly on safety-related subsystems – to be detected and prevented.

When designing and manufacturing a vehicle, the future data processing has to take the principles of "privacy by design" and "privacy by default" into account. Personal data should principally remain within the car itself and only be anonymously or pseudonymously processed on the backend server of the manufacturers or service providers. The requirements on data protection should be tested at the time of the type-approval of the vehicle, as is the case with eCall. Web service providers should provide evidence of meeting these requirements by proving a corresponding audit or a certification of their data protection guidelines.

[1] ECJ judgement "Patrick Beyer vs. Federal Republic of Germany"(C 582/14), 2016-10-16

4. TÜV-Approach: Automotive platform

Connected and automated vehicle systems have to comply with IT-requirements against cyberattacks on the one side and the protection of intellectual property as well as the legal data protection requirements mentioned above on the other side.

In the future, a highly secure communication platform, installed in all vehicles as standard, could be implemented in order to meet the requirements on data protection and IT security of these new technologies and business models. This central platform shall connect all the electronic control devices in the different domains of the vehicle. These include the drive train, driver assistance systems, infotainment services as well as the chassis and comfort electronics. The platform is also the central point of access for carrying out software updates as well as diagnostics and maintenance tasks via the on-board diagnostics (OBD). At the same time, the platform securely separates the services (the vehicle's external interface) from the information systems relevant to the driver (driver domain) and from the safety-related components (safety domain). Any information leaving the vehicle shall be processed in advance by the embedded platform in accordance with specific user profiles. The same applies for any information entering the vehicle.

This communication platform would create a uniform and interoperable standard for security and safety in the vehicle, which provides for, among other things, the following security features (security by design):

- Information flow control (firewall)
- Identification / authentication
- Access control to the vehicle interface
- Auditing
- Random number generator
- Encryption (cryptographic signing method)

An assessed hardware security module should be used for the encryption methods and random number generator.

Such a platform shall process data content in accordance with vehicle profiles which are to be defined. Following the allocation of the data, it shall send the data – signed and encrypted – to different service providers (OEMs, supplier, insurance company, owner, fleet management, emergency service, smart city services, car parks, warning services, testing authorities, etc.). The vehicle profiles can be modified by an administrator while not having any direct read access to the data.

With this process, the privacy by design approach is applied. Only data which are classified to be transmitted for a specific purpose shall be exchanged according to the General Data Protection Regulation. In the vehicle's delivery state, the platform shall be set to the "highest data protection level" (privacy by default). Should the vehicle users/owners give their consent, their personal data can be transmitted for other purposes of use; this shall then be mapped in the user profiles.

VdTÜV recommends that a highly-secure communication platform - as described above - shall be specified and implemented. This platform shall technologically implement the data and consumer protection of the vehicle occupants in a flexible manner. At the same time, it should be apt for the different third party requirements and serve as their communication basis.

Protection from manipulation of the vehicle software as well as of the internal and external data traffic is being improved. Communication protocols and services which have already been defined by the automotive industry are continuing to be observed and used, provided that they do not conflict with the security architecture.

A European legislative initiative can enforce strict data protection provisions for the development of such a data exchange system which is in the interest of the consumer, and will also improve the compatibility of connected vehicles in the European Single Market through uniform standards across Europe.